PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :
H04L 9/32, G07F 7/10

A1

(11) International Publication Number: **WO 93/07697**

(43) International Publication Date: 15 April 1993 (15.04.93)

(21) International Application Number: PCT/SE92/00656

(22) International Filing Date: 23 September 1992 (23.09.92)

(30) Priority data:
9102835-7 30 September 1991 (30.09.91) SE

(71) Applicant *(for all designated States except US)*: COMVIK GSM AB [SE/SE]; P.O. Box 123, S-126 23 Hägersten (SE).

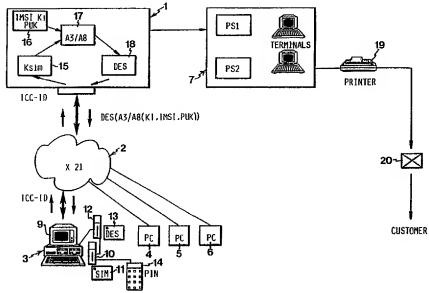
(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : JULIN, Tomas [SE/SE]; Andvägen 32, S-184 61 Åkersberga (SE). ALMGREN, Björn [SE/SE]; Svartvikslingan 87, S-161 29 Bromma (SE). SANDBERG, Leif [SE/SE]; Jäntans väg 14, S-132 35 Saltsjö-Boo (SE).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S-104 30 Stockholm (SE).

(81) Designated States: AU, CA, FI, JP, NO, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE).

Published
With international search report.

(54) Title: METHOD FOR PERSONALISATION OF AN ACTIVE CARD



(57) Abstract

Personalisation of an active so-called SIM card (11) for a mobile telephone system of GSM type is effected in a place (3) connected to the central computer (1) of the system via a communication network (2). The card identity IMSI and the card authentication key Ki are transferred in line-encrypted form (DES) to terminal equipment (9) in said place, where the card (11) is inserted in a reader (10). After line decryption (12, 13), the result thereof is transferred to the card in a manner to prevent unauthorised listening-in. This can be done in a safety box or by double encryption (A3/A8) of IMSI and Ki, the decryption thereof being performed within the card by means of a unique card key Ksim.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NL	Netherlands
BE	Belgium	GN	Guinea	NO	Norway
BF	Burkina Faso	GR	Greece	NZ	New Zealand
BG	Bulgaria	HU	Hungary	PL	Poland
BJ	Benin	IE	Ireland	PT	Portugal
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SK	Slovak Republic
CI	Côte d'Ivoire	LI	Liechtenstein	SN	Senegal
CM	Cameroon	LK	Sri Lanka	SU	Soviet Union
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	MC	Monaco	TG	Togo
DE	Germany	MG	Madagascar	UA	Ukraine
DK	Denmark	ML	Mali	US	United States of America
ES	Spain	MN	Mongolia	VN	Viet Nam
FI	Finland				

TITLE OF THE INVENTION

Method for personalisation of an active card

TECHNICAL FIELD

The present invention relates to a method for personalisation of an active subscriber card, a so-called SIM card, for use in a mobile telephone system, comprising a central computer, the unique identity of the card, so-called IMSI, and the unique authentication key of the card, so-called Ki, being stored in the card from the central computer. The invention is especially applicable to a mobile telephone system of GSM type and will be described in more detail with reference thereto, although it is obvious that the invention is also applicable to other mobile telephone systems of similar type.

TECHNICAL BACKGROUND

In mobile telephone systems, in which the mobile units are controlled by active cards assigned to the subscribers, the personalisation of the respective card constitutes an essential procedure which is safeguarded by rigorous security measures and which includes activating the card and loading it with IMSI and Ki, and preferably also a so-called PUK code (Personal Unblocking Key). It is essential that this loading be effected in a safe manner to prevent unauthorised people from having access thereto.

In view hereof, the personalisation procedure is carried out in a central personalisation place or a customer service place adjacent the central computer, where it is possible to meet the high demands on security.

OBJECT OF THE INVENTION

The object of the present invention is to provide a method making it possible, still in a safe manner, to effect the personalisation procedure in other places than the above-mentioned central place, whereby a number of advantages can be gained.

SUMMARY OF THE INVENTION

The above-mentioned object is achieved by a method which according to the invention has the features stated in the appended claims.

According to the invention, the storage procedure should thus be carried out when the card is in a personalisation place remotely connected to the central computer via a data communication network, especially a retail place, the card being inserted in a reader associated with data terminal equipment connected to the data communication network, IMSI and Ki and preferably also PUK being transferred in line-encrypted form from the central computer to the data terminal equipment where line decryption is performed, and the result of the line decryption being transferred to the SIM card in a manner to prevent unauthorised listening-in.

A distributed personalisation of this type makes it possible to divide up IMSI number series geographically, which is a major advantage in that the network signalling is simplified or reduced, and also in that the service level towards a new subscriber can be kept very high. In fact, the personalisation can be effected directly and without any waiting times conditioned by the dispatch of cards, code envelopes etc., from a central place. The direct communication with the central computer also makes it possible to provide for different special services in a rapid and simple manner.

The transfer of the result of the line decryption to the SIM card in a safe manner can be carried out in different ways.

According to a first conceivable alternative, the line decryption and the result transfer to the SIM card take place in a physically sealed space, into which any attempt of unauthorised intrusion means that relevant information is erased and that the process is interrupted and cannot be continued without special security measures being taken. Mechanical and electronic protection of this

kind can be achieved by means of a special safety box, in which the circuitry concerned is enclosed during the personalisation procedure.

According to a second conceivable alternative, the result of the line decryption is transferred to the SIM card in encrypted form, at least in respect of Ki. This is preferably done by encrypting Ki and preferably also PUK and optionally IMSI an extra time in the central computer before the line-encrypted transfer to the personalisation place, the result of the line decryption transferred to the SIM card being decrypted within the SIM card by means of a card key Ksim, which has suitably been stored in the SIM card in connection with the manufacture thereof. This card key Ksim is preferably unique to the respective card.

The decryption in the SIM card here takes place advantageously by means of the card key and a secret algorithm, especially being the algorithm which is intended for encryption/decryption in connection with the regular use of the card in the mobile telephone system, and on which there is information in the central computer. Advantageously, the algorithm is of type A3/A8 according to GSM recommendation.

According to the invention, it is preferred that the central computer before the double encryption calculates the required Ksim, using SIM-card identification transferred from the personalisation place, the "master key" by means of which the SIM card is manufactured and the pertaining algorithm.

It is understood that the central computer may have been separately supplied with information on both said master key and the algorithm concerned for new SIM cards after the manufacture thereof with the card manufacturer.

It is however also possible that the above-mentioned SIM-card identification transferred to the central computer may contain such information that the central computer can conclude on the basis thereof which master key

(among a number of possible ones) and which algorithm (among a number of possible ones) are at issue.

This obviously means that the key Ksim, for enhanced security, can be modified during the continuous manufacture of the SIM cards.

The above-mentioned SIM-card identification may consist of the serial number of the card, which then can include special fields with information on e.g. master key and/or the algorithm concerned.

It is understood that, for further enhanced security, it is possible to combine the two alternatives described above.

According to the invenion, it is further advantageous to control the personalisation procedure by means of an active personalisation card which is inserted in a reader associated with the data terminal equipment and which contains at least parts of the line-encryption function, especially a pertaining key, preferably also the pertaining algorithm.

Anyone who handles the personalisation procedure (e.g. a retailer) can thus have his own unique active card, which can thus be used both for authorisation checks (active and passive authentication), and as an encrypting unit. Everybody can then have an individual encryption key for further enhanced security.

Further features of the invention will appear from the following description of exemplifying embodiments with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagrammatical general view illustrating an embodiment of the method according to the invention.

Fig. 2 is a block diagram which illustrates in more detail the embodiment of Fig. 1.

Fig. 3 is a block diagram illustrating another embodiment of the method according to the invention.

DESCRIPTION OF EMBODIMENTS

In Fig. 1, reference number 1 designates, in a mobile telephone system, a central computer which via a data communication network 2 communicates with a number of retailers 3, 4, 5, 6, and which also communicates with a customer service place 7.

Each retailer has data terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line-encryption equipment 12, 13 consisting of a reader 12 and an active retailer card 13. A keyboard 14 for entering a PIN code in a SIM card concerned is connected to the reader 10.

The central computer 1 contains means 15 for calculating Ksim on the basis of card information ICC-ID transferred from the retailer place, means 16 for generating IMSI, Ki and PUK, means 17 for encrypting the latter ones, using the key Ksim and an A3/A8 algorithm, and means 18 for DES line encryption.

The central computer provides information about PUK to the customer service place 7, which on a printer 19 prints out a letter 20 with information about this. This letter is sent by post to the customer concerned.

The function according to the invention will now be described in more detail with reference also to Fig. 2.

The systems operator 21 informs the card manufacturer 22 and the central computer 1 about master key, DES and A3/A8 algorithms, and the central computer also about the retailer card key Kl. The card manufacturer calculates Ksim for the respective card in a series to be sent to a certain retailer 3 based on the DES algorithm, the master key and the card serial number. Ksim and the A3/A8 algorithm are loaded in the card along with card serial numbers before the card is sent to the retailer.

From the systems operator, the retailer receives his personal active card 13 with the pertaining entered card key Kl and DES algorithm for the line encryption, about which the central computer thus holds information.

When a retailer is to personalise a new SIM card for a new subscriber, he starts by inserting his active card 13 in a reader 12 associated with the retailer terminal and logs in in customary manner, the active card serving as authentication means (optionally together with a PIN code which is unique to the retailer and which is inputted on the terminal keyboard), thus verifying the authorisation of the retailer.

A new SIM card 11 is now inserted in the pertaining reader 10, card-indentifying information ICC-ID being transferred from certain fields, preprogrammed during the manufacture of the card, in the SIM card via the retailer terminal 9 and the network 2 to the central computer 1. Other relevant subscriber data are inputted via the keyboard of the terminal and transmitted to the central computer for customary checking, etc. If the subscriber is accepted, the number MSISDN selected or accepted by the subscriber is also transmitted to the central computer.

In the central computer, Ksim is calculated on the basis of the information received on master key, serial number and DES algorithm. Ki and PUK are generated as random numbers. IMSI is allocated from the IMSI series prepared for the retailer or the area to which the retailer belongs.

IMSI, Ki and PUK are encrypted using Ksim and the selected A3/A8 algorithm. The thus-encrypted IMSI, Ki and PUK and other data to be transferred are thereafter line encrypted using the key K1 and the DES algorithm, and transferred via the data communication network to the retailer terminal, where line decryption occurs using the card key K1 and DES algorithm of the retailer's active card 13.

Via the reader 10, the other data now decrypted can be loaded directly in the SIM card, while IMSI, Ki and PUK, still in encrypted form, are transferred to the SIM card for decryption therein, using the card key Ksim and the pertaining A3/A8 algorithm. Advantageously, this algo-

rithm is identical with the algorithm which is intended for the regular use of the card and which is unique to the systems operator and can be varied for different card series, if desired.

After decryption, IMSI, Ki and PUK are loaded in the pertaining data field in the SIM card.

Via the PIN keyboard 13, the subscriber can himself load an optional PIN code in the SIM card in a strictly confidential manner. The card is thus ready for use. The PUK code assigned by the central computer is sent to the subscriber by post after a day or two.

The alternative embodiment of the invention shown in Fig. 3 differs from that in Figs 1 and 2 by the absence of the double encryption procedure. The transfer of Ki, IMSI and PUK to the SIM card 11 after line decryption, which occurs by means of the retailer card 13 inserted in its reader 12, instead occurs in a protected manner, by the card reader 12 with its card 13 and the SIM card 11 in its reader 10 (connected to the reader 12) being mechanically and electronically protectively enclosed in a safety box 31 during the personalisation procedure.

As readily appreciated by those skilled in the art, the safety box 31 may be designed in many different ways, which also applies to the means which should be provided for interrupting the procedure and erasing sensitive data in the case of an attempted intrusion into the safety box.

It is understood that the two alternatives described above can be combined, if additional security is desired in the retailer place and/or during the transfer via the data communication network.

CLAIMS

1. Method for personalisation of an active card, a so-called SIM card, for use in a mobile telephone system, especially of GSM type, comprising a central computer, the unique identity of the card, so-called IMSI, and the unique authentication key of the card, so-called Ki, being stored in the card from the central computer, c h a r - a c t e r i s e d by carrying out the storage procedure when the card is in a personalisation place remotely connected to the central computer via a data communication network, e.g. a retail place, the card being inserted in a reader associated with data terminal equipment connected to the data communication network; transferring IMSI and Ki in line-encrypted form from the central computer to the data terminal equipment, where line decryption occurs; and transferring the result of the line decryption to the SIM card in a manner to prevent unauthorised listening-in, at least in respect of Ki.

2. Method as claimed in claim 1, c h a r a c t e r - i s e d in that the line decryption and the result transfer to the SIM card are performed in a physically sealed space, such as a safety box, into which any attempt of unauthorised intrusion results in the erasure of relevant information.

3. Method as claimed in claim 1 or 2, c h a r a c - t e r i s e d in that the result of the line decryption is transferred in encrypted form to the SIM card.

4. Method as claimed in claim 3, c h a r a c t e r - i s e d in that Ki and preferably also IMSI are double-encrypted in the central computer before the transfer to the personalisation place, the result of the line decryption transferred to the SIM card being decrypted in the SIM card by means of a card key Ksim, which has preferably been stored in the SIM card in connection with the manufacture thereof.

5. Method as claimed in claim 4, characterised in that the decryption in the SIM card is performed by means of a key Ksim unique to the card, and an algorithm intended for the regular use of the card.

6. Method as claimed in claim 5, characterised in that the central computer, before the encryption, calculates Ksim, using SIM-card identification transferred from the personalisation place, the master key with which the SIM card is produced and on which information has been entered in the central computer, and the pertaining algorithm.

7. Method as claimed in any one of the preceding claims, characterised in that it is controlled by means of an active personalisation card which is inserted in a reader pertaining to the data terminal equipment and which contains at least parts of the line-encryption function.

8. Method as claimed in claim 7, characterised in that use is made of a personalisation card with a DES algorithm.

9. Method as claimed in claim 2 and claim 7 or 8, characterised in that the two readers and the path of communication therebetween are placed in said physically sealed space.

10. Method as claimed in any one of the preceding claims, characterised in that a so-called PIN code is stored in the active SIM card by means of a keyboard pertaining to the data terminal equipment.

11. Method as claimed in any one of the preceding claims, characterised in that a so-called PUK code is transferred from the central computer to the SIM card in the same way as defined for Ki.

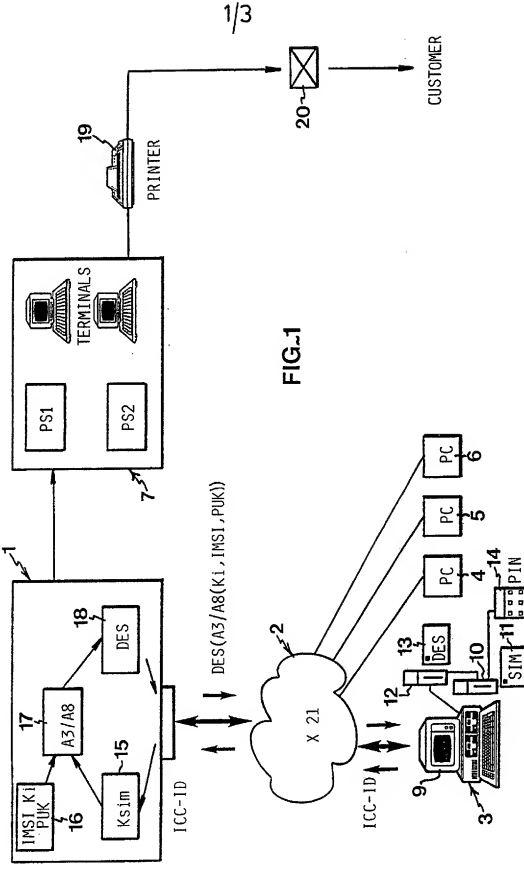

1
IMSI Ki PUK
16
A3/A8
17
Ksim
15
DES
18
ICC-ID
DES(A3/A8(Ki, IMSI, PUK))
2
X 21
ICC-ID
9
3
12
13
DES
10
SIM
11
PC
4
PC
5
PC
6
14
PIN
PS1
PS2
TERMINALS
7
19
PRINTER
20
CUSTOMER

FIG.1

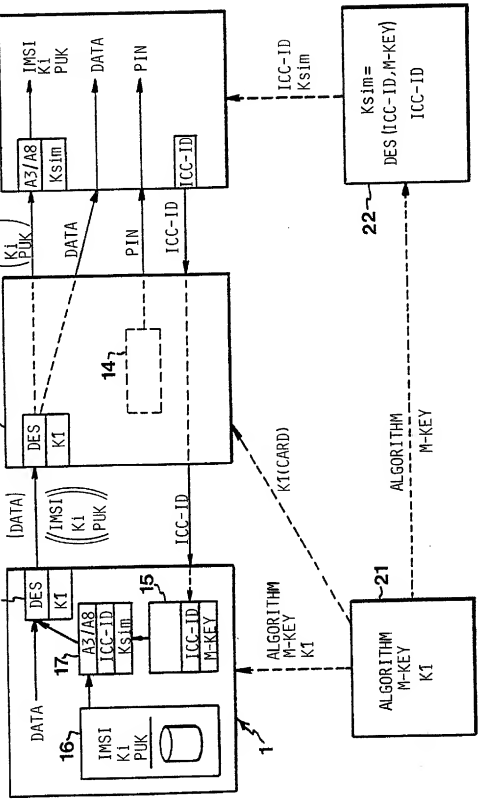

10,11
IMSI
K1
PUK
DATA
PIN
ICC-ID
A3/A8
Ksim
ICC-ID
Ksim
Ksim=
DES [ICC-ID,M-KEY)
ICC-ID
22
9,12,13
DES
K1
14
(IMSI
K1
PUK)
DATA
PIN
ICC-ID
K1(CARD)
ALGORITHM
M-KEY
18
DES
K1
17
A3/A8
ICC-ID
Ksim
15
ICC-ID
M-KEY
16
IMSI
K1
PUK
DATA
[DATA]
(IMSI
K1
PUK)
ICC-ID
ALGORITHM
M-KEY
K1
21
ALGORITHM
M-KEY
K1
1

FIG_2

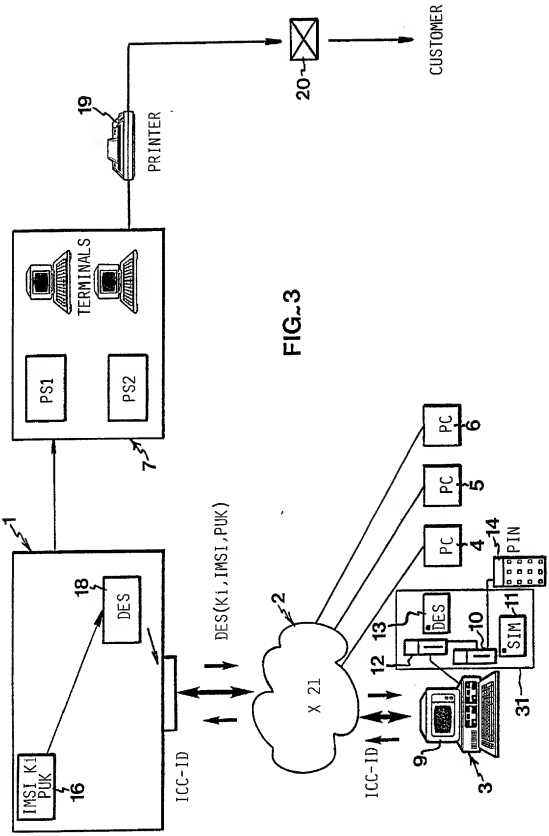

CUSTOMER
20
19
PRINTER
TERMINALS
PS1
PS2
7
1
18
DES
IMSI Ki
PUK
16
ICC-ID
DES(Ki,IMSI,PUK)
2
X 21
PC
6
PC
5
PC
4
14
PIN
13
DES
12
10
SIM
11
ICC-ID
9
3
31

FIG.3

INTERNATIONAL SEARCH REPORT

International Application No PCT/SE 92/00656

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC5: H 04 L 9/32, G 07 F 7/10

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
IPC5	G 06K; G 07 C; G 07 F; H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in Fields Searched[8]

SE,DK,FI,NO classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category *	Citation of Document,[11] with indication, where appropriate, of the relevant passages[12]	Relevant to Claim No.[13]
A	US, A, 5012074 (SHIGEO MASADA) 30 April 1991, see column 2, line 28 - column 5, line 17 --	1-11
A	US, A, 5020105 (RICHARD D. ROSEN ET AL) 28 May 1991, see column 2, line 62 - column 3, line 17; column 6, line 4 - column 7, line 12 --	1-11
A	WO, A1, 8903143 (APPLIED INFORMATION TECHNOLOGIES RESEARCH CENTER) 6 April 1989, see page 14, line 10 - page 21, line 25 --	1-11

---

* Special categories of cited documents:[10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
18th December 1992	23 -12- 1992
International Searching Authority	**Signature of Authorized Officer**
SWEDISH PATENT OFFICE	BO GUSTAVSSON

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. PCT/SE 92/00656

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the Swedish Patent Office EDP file on 02/12/92
The Swedish Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 5012074	91-04-30	DE-A-C- 3809170	88-10-13
		FR-A- 2613102	88-09-30
		JP-A- 63236186	88-10-03
US-A- 5020105	91-05-28	AU-D- 8078587	89-04-18
		US-A- 4731841	88-03-15
		WO-A- 89/03143	89-04-06
WO-A1- 8903143	89-04-06	AU-D- 8078587	89-04-18
		US-A- 4731841	88-03-15
		US-A- 5020105	91-05-28